Risk Analysis

for

Payload Launch Control Simulator

Version 1.0

James Furtado

1. Purpose

This document outlines potential risks that could affect the development and use of the Payload Launch Control Simulator (PLCS). Its goal is to help catch problems early and ensure the system stays reliable and safe throughout the project development lifecycle.

2. Risk Assessment Table

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Mitigation Strategy
R-1	Launch command is accepted while safety constraints are violated. (FR-3)	Medium	High	High	Implement in-depth safety checks (assertions and fail-safe defaults).
R-2	UI does not obviously show safety or environmental state. (FR-4, FR-6, NFR-3)	Medium	Medium	Medium	Use color-coded indicators and real-time updates.
R-3	Simulation engine state exhibits invalid behavior due to errors in update or reset logic. (FR-5, FR-8, FR-9)	Low	High	Medium	Design a clear state machine block diagram, write automated tests alongside development.
R-4	Delay in command response exceeds real-time constraint. (NFR-1)	Low	Low	Low	Optimize UI and backend logic.
R-5	Simulation does not exhibit realistic environment and system behaviors. (FR-5)	High	Medium	Medium	Allow configurable environment/system parameters.
R-6	Incomplete test coverage allows bugs to pass through. (NFR-4)	Medium	Medium	Medium	Write testing docs and incorporate edge cases with uncommon scenarios.
R-7	Operator confusion during operation due to unclear flow. (NFR-3, FR-1, FR-2)	Medium	Medium	Medium	Include instructions for operator usage in the UI.